Attorney Docket No.: 0918.0011C

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the PATENT application of

Edwin H. Wrench, Jr.

Serial No.: 09/731,836	Group Art Unit: 2137
Filed: December 8, 2000	Examiner: Pyzocha, Michael J.
Technology Center: 2100	Confirmation No.: 1865

For: Method and Apparatus to Facilitate Secure Network Communications with a Voice Responsive Network Interface Device

RESPONSE TO NOTIFICATION OF NON-COMPLIANT APPEAL BRIEF

MAIL STOP APPEAL BRIEF-PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Pursuant to the Notification of Non-Compliant Appeal Brief mailed August 21, 2006, the following revised section (Summary of Claimed Subject Matter) of the Appeal Brief filed August 2, 2006 is submitted in accordance with M.P.E.P. §1205.03.

(5) Summary of Claimed Subject Matter

Independent claim 1 is directed toward a system for facilitating secure encrypted communications over a network with a network interface configured to provide unencrypted sessions with web sites and including a voice browser (e.g., See Fig. 1; Specification Page 8, Lines 22 - 28; and Page 17, Lines 25 - 27). The system comprises: a security module for the network interface (e.g., See Figs. 1, 4 and 7, security module 6; Specification Page 5, Lines 24 - 25; Page 8, Lines 25 - 28; Page 9, Lines 16 - 22; and Page 12, Lines 21 - 25) that facilitates retrieval of information from the user in the form of voice signals (e.g., See Figs. 1, 2 (e.g., step 44), 3 (e.g., steps 74 and 76) and 4 (e.g., flow 96); Specification Page 5, Lines 27 - 31; Page 10, Line 27 to Page 11, Line 2; Page 12, Lines 8 - 12 and 28 - 31), detects a secure web server providing encrypted sessions (e.g., See Figs. 1, 5 (e.g., step 122), 6 (e.g., step 130) and 7; Specification Page 6, Lines 2 - 4; Page 14, Line 30 to Page 15, Line 6), and identifies security related information received by the network interface from the secure web server in response to the voice browser accessing a secure web site of the secure web server based on voice commands from the user (e.g., See Figs. 1, 5 (e.g., step 122), 6 (e.g., step 130) and 7; Specification Page 6, Lines 2 - 7; Page 14, Line 30 to Page 15, Line 6), wherein the security related information includes information enabling a secure encrypted session with the secure web server (e.g., See Specification Page 6, Lines 2 - 7; and Page 13, Lines 7 - 13); a storage unit to store remote from the network interface voice and security information associated with authorized users of the system (e.g., See Figs. 1 (database 8), 3 (e.g., steps 72, 78 and 84), and 4 (e.g., flows 102 and 118); Specification Page 5, Line 27 to Page 6, Line 2; Page 11, Lines 2 - 6 and 24 - 26; Page 12, Lines 12 - 19; and Page 13, Lines 3 - 7), wherein the security information includes information enabling negotiation of parameters for secure encrypted sessions with secure web servers (e.g., See Specification Page 5, Line 31 to Page 6, Line 2; Page 11, Lines 2 - 6 and 11 - 13; Page 12, Lines 17 - 19; and Page 13, Lines 3 - 7); and a security system to communicate with the security module and the storage unit and to process for the network interface the identified security information to enable the secure encrypted session (e.g., See Figs. 1, 4 and 7, security system 4; Specification Page 5, Lines 20 - 23; Page 6, Lines 4 - 10; and Page 7, Lines 20 - 22). The security system includes: a verification module to verify the user as an authorized system user based on a comparison of the user voice signals with the stored voice information (e.g., See Figs. 1, 2 (e.g., step 46), 3 (e.g., step 78), and 4 (e.g., flow 112); Specification Page 5, Lines 27 - 31; Page 10, Line 27 to Page 11, Line 2; Page 11, Lines 24 - 26; Page 12, Lines 8 - 17; and Page 12, Line 28 to Page 13, Line 3); a retrieval module to retrieve the security information of the verified user from the storage unit (e.g., See Figs. 3 (e.g., step 84) and 4 (e.g., flow 118); Specification Page 5, Line 31 to Page 6, Line 2; Page 11, Lines 2 - 6 and 11 - 13; Page 12, Lines 17 - 19; and Page 13, Lines 3 - 7); and a negotiation module to receive the identified security information from the security module and negotiate communication parameters with the secure web server utilizing the retrieved security information to facilitate the secure encrypted session between the secure web server and the voice browser (e.g., See Figs. 1, 5 - 7; Specification Page 6, Lines 2 - 10; Page 14, Line 30 to Page 15, Line 26; and Page 16, Lines 4 - 14).

Independent claim 12 is directed toward a program product apparatus having a computer readable medium with computer program logic recorded thereon for facilitating secure encrypted communications over a network with a network interface configured to provide unencrypted sessions with web sites and including a voice browser (e.g., See Fig. 1; Specification Page 8, Lines 22 - 28; Page 17, Lines 25 - 27; and Page 18, Line 29 to Page 19, Line 3). The apparatus comprises: a security module for the network interface (e.g., See Figs. 1, 4 and 7, security module 6; Specification Page 5, Lines 24 - 25; Page 8, Lines 25 - 28; Page 9, Lines 16 - 22; and Page 12, Lines 21 - 25) that facilitates retrieval of information from the user in the form of voice signals (e.g., See Figs. 1, 2 (e.g., step 44), 3 (e.g., steps 74 and 76) and 4 (e.g., flow 96); Specification Page 5, Lines 27 - 31; Page 10, Line 27 to Page 11, Line 2; Page 12, Lines 8 - 12 and 28 - 31), detects a secure web server providing encrypted sessions (e.g., See Figs. 1, 5 (e.g., step 122), 6 (e.g., step 130) and 7; Specification Page 6, Lines 2 - 4; Page 14, Line 30 to Page 15, Line 6), and identifies security related information received by the network interface from the secure web server in response to the voice browser accessing a secure web site of the secure web server based on voice commands from the user (e.g., See Figs. 1, 5 (e.g., step 122), 6 (e.g., step 130) and 7; Specification Page 6, Lines 2 - 7; Page 14, Line 30 to Page 15, Line 6), wherein the security related information includes information enabling a secure encrypted session with the secure web server (e.g., See Specification Page 6, Lines 2 - 7; and Page 13, Lines 7 - 13); a storage module to store remote from the network interface voice and security information associated with authorized users (e.g., See Figs. 1, 3 (e.g., steps 72, 78 and 84), and 4 (e.g., flows 102 and 118); Specification Page 5, Line 27 to Page 6, Line 2; Page 11, Lines 2 - 6 and 24 - 26; Page 12, Lines 12 - 19; and Page 13, Lines 3 - 7), wherein the security information includes information enabling negotiation of parameters for secure encrypted sessions with secure web servers (e.g., See Specification Page 5, Line 31 to Page 6, Line 2; Page 11, Lines 2 - 6 and 11 - 13; Page 12, Lines 17 - 19; and Page 13, Lines 3 - 7); and a secure communications module for a security system to communicate with the security module and the storage module and to process for the network interface the identified security information to enable the secure encrypted session (e.g., See Figs. 1, 4 and 7, security system 4; Specification Page 5, Lines 20 - 23; Page 6, Lines 4 - 10; and Page 7, Lines 20 - 22). The secure communications module includes: a verification module to verify the user as an authorized system user based on a comparison of the user voice signals with the stored voice information (e.g., See Figs. 1, 2 (e.g., step 46), 3 (e.g., step 78), and 4 (e.g., flow 112); Specification Page 5, Lines 27 - 31; Page 10, Line 27 to Page 11, Line 2; Page 11, Lines 24 - 26; Page 12, Lines 8 - 17; and Page 12, Line 28 to Page 13, Line 3); a retrieval module to retrieve the security information of the verified user from the storage module (e.g., See Figs. 3 (e.g., step 84) and 4 (e.g., flow 118); Specification Page 5, Line 31 to Page 6, Line 2; Page 11, Lines 2 - 6 and 11 - 13; Page 12, Lines 17 - 19; and Page 13, Lines 3 - 7); and a negotiation module to receive the identified security information from the security module and negotiate communication parameters with the secure web server utilizing the retrieved security information to facilitate the secure encrypted session between the secure web server and the voice browser (e.g., See Figs. 1, 5 - 7; Specification Page 6, Lines 2 - 10; Page 14, Line 30 to Page 15, Line 26; and Page 16, Lines 4 - 14).

Independent claim 16 is directed toward a carrier signal having computer program logic embedded therein causing an apparatus to facilitate secure encrypted communications over a network with a network interface configured to provide unencrypted sessions with web sites and including a voice browser (e.g., See Fig. 1; Specification Page 8, Lines 22 - 28; Page 17, Lines 25 - 27; and Page 18, Line 29 to Page 19, Line 3). The carrier signal comprises: a security module for the network interface (e.g., See Figs. 1, 4 and 7, security module 6; Specification Page 5, Lines 24 - 25; Page 8, Lines 25 - 28; Page 9, Lines 16 - 22; and Page 12, Lines 21 - 25) that facilitates retrieval of information from the user in the form of voice signals (e.g., See Figs. 1, 2 (e.g., step 44), 3 (e.g., steps 74 and 76) and 4 (e.g., flow 96); Specification Page 5, Lines 27 - 31; Page 10, Line 27 to Page

11, Line 2; Page 12, Lines 8 - 12 and 28 - 31), detects a secure web server providing encrypted sessions (e.g., See Figs. 1, 5 (e.g., step 122), 6 (e.g., step 130) and 7; Specification Page 6, Lines 2 - 4; Page 14, Line 30 to Page 15, Line 6), and identifies security related information received by the network interface from the secure web server in response to the voice browser accessing a secure web site of the secure web server based on voice commands from the user (e.g., See Figs. 1, 5 (e.g., step 122), 6 (e.g., step 130) and 7; Specification Page 6, Lines 2 - 7; Page 14, Line 30 to Page 15, Line 6), wherein the security related information includes information enabling a secure encrypted session with the secure web server (e.g., See Specification Page 6, Lines 2 - 7; and Page 13, Lines 7 - 13); a storage module to store remote from the network interface voice and security information associated with authorized users (e.g., See Figs. 1, 3 (e.g., steps 72, 78 and 84), and 4 (e.g., flows 102 and 118); Specification Page 5, Line 27 to Page 6, Line 2; Page 11, Lines 2 - 6 and 24 - 26; Page 12, Lines 12 - 19; and Page 13, Lines 3 - 7), wherein the security information includes information enabling negotiation of parameters for secure encrypted sessions with secure web servers (e.g., See Specification Page 5, Line 31 to Page 6, Line 2; Page 11, Lines 2 - 6 and 11 - 13; Page 12, Lines 17 - 19; and Page 13, Lines 3 - 7); and a secure communications module for a security system to communicate with the security module and the storage module and to process for the network interface the identified security information to enable the secure encrypted session (e.g., See Figs. 1, 4 and 7, security system 4; Specification Page 5, Lines 20 - 23; Page 6, Lines 4 - 10; and Page 7, Lines 20 - 22). The secure communications module includes: a verification module to verify the user as an authorized system user based on a comparison of the user voice signals with the stored voice information (e.g., See Figs. 1, 2 (e.g., step 46), 3 (e.g., step 78), and 4 (e.g., flow 112); Specification Page 5, Lines 27 - 31; Page 10, Line 27 to Page 11, Line 2; Page 11, Lines 24 - 26;

Page 12, Lines 8 - 17; and Page 12, Line 28 to Page 13, Line 3); a retrieval module to retrieve the security information of the verified user from the storage module (e.g., See Figs. 3 (e.g., step 84) and 4 (e.g., flow 118); Specification Page 5, Line 31 to Page 6, Line 2; Page 11, Lines 2 - 6 and 11 - 13; Page 12, Lines 17 - 19; and Page 13, Lines 3 - 7); and a negotiation module to receive the identified security information from the security module and negotiate communication parameters with the secure web server utilizing the retrieved security information to facilitate the secure encrypted session between the secure web server and the voice browser (e.g., See Figs. 1, 5 - 7; Specification Page 6, Lines 2 - 10; Page 14, Line 30 to Page 15, Line 26; and Page 16, Lines 4 - 14).

Independent claim 20 is directed toward a method of facilitating secure encrypted communications over a network with a network interface configured to provide unencrypted sessions with web sites and including a voice browser (e.g., See Fig. 1; Specification Page 8, Lines 22 - 28). The method comprises: (a) retrieving, via a security module (e.g., See Figs. 1, 4 and 7, security module 6; Specification Page 5, Lines 24 - 25; Page 8, Lines 25 - 28; Page 9, Lines 16 - 22; and Page 12, Lines 21 - 25), information from the user in the form of voice signals (e.g., See Figs. 1, 2 (e.g., step 44), 3 (e.g., steps 74 and 76) and 4 (e.g., flow 96); Specification Page 5, Lines 27 - 31; Page 10, Line 27 to Page 11, Line 2; Page 12, Lines 8 - 12 and 28 - 31) and detecting a secure web server providing encrypted sessions (e.g., See Figs. 1, 5 (e.g., step 122), 6 (e.g., step 130) and 7; Specification Page 6, Lines 2 - 4; Page 14, Line 30 to Page 15, Line 6) and identifying security related information received by the network interface from the secure web server in response to the voice browser accessing a secure web site of the secure web server based on voice commands from the user (e.g., See Figs. 1, 5 (e.g., step 122), 6 (e.g., step 130) and 7; Specification Page 6, Lines 2 - 7; Page 14, Line 30 to Page 15, Line 6), wherein the security related information includes information enabling a secure encrypted session with the secure web server (e.g., See Specification Page 6, Lines 2 - 7; and Page 13, Lines 7 - 13); (b) storing remote from the network interface voice and security information associated with authorized users in a storage unit (e.g., See Figs. 1 (database 8), 3 (e.g., steps 72, 78 and 84), and 4 (e.g., flows 102 and 118); Specification Page 5, Line 27 to Page 6, Line 2; Page 11, Lines 2 - 6 and 24 - 26; Page 12, Lines 12 - 19; and Page 13, Lines 3 - 7), wherein the security information includes information enabling negotiation of parameters for secure encrypted sessions with secure web servers (e.g., See Specification Page 5, Line 31 to Page 6, Line 2; Page 11, Lines 2 - 6 and 11 - 13; Page 12, Lines 17 - 19; and Page 13, Lines 3 - 7); (c) verifying the user as an authorized system user based on a comparison of the user voice signals with the stored voice information (e.g., See Figs. 1, 2 (e.g., step 46), 3 (e.g., step 78), and 4 (e.g., flow 112); Specification Page 5, Lines 27 - 31; Page 10, Line 27 to Page 11, Line 2; Page 11, Lines 24 - 26; Page 12, Lines 8 - 17; and Page 12, Line 28 to Page 13, Line 3) via a security system (e.g., See Figs. 1, 4 and 7, security system 4; Specification Page 5, Lines 20 - 23; Page 6, Lines 4 - 10; and Page 7, Lines 20 - 22); (d) retrieving, via the security system, the security information of the verified user from the storage unit (e.g., See Figs. 3 (e.g., step 84) and 4 (e.g., flow 118); Specification Page 5, Line 31 to Page 6, Line 2; Page 11, Lines 2 - 6 and 11 - 13; Page 12, Lines 17 - 19; and Page 13, Lines 3 - 7); and (e) receiving the identified security information from the security module at the security system and negotiating communication parameters for the network interface with the secure web server utilizing the retrieved security information to facilitate the secure encrypted session between the secure web server and the voice browser (e.g., See Figs. 1, 5 - 7; Specification Page 6, Lines 2 - 10; Page 14, Line 30 to Page 15, Line 26; and Page 16, Lines 4 - 14).

REMARKS

The Notification of Non-Compliant Appeal Brief indicated that the Summary of the Claimed Invention section of the Appeal Brief filed August 2, 2006 does not contain a mapping of independent claims 1, 12, 16, 17 and 20 to the specification. However, since claim 17 is a dependent claim, the Summary of the Claimed Invention section of the Appeal Brief has been revised in accordance with the notification with respect to independent claims 1, 12, 16 and 20. Accordingly, the Appeal Brief is considered to comply with appropriate requirements.

Respectfully submitted,

Stuart B. Shap

Stuart B. Shapiro
Registration No. 40,169

EDELL, SHAPIRO & FINNAN, LLC
1901 Research Boulevard, Suite 400
Rockville, Maryland 20850
(301) 424-3640

Electronically Delivered: 9/13/2006